COPY 1 of 1 COPIES

CONCERNING COMPOUND RANDOMIZATION IN THE BINARY SYSTEM

John E. Walsh

P 10

Revised June 21, 1949

The RAND Corporation
1700 MAIN ST. • SANTA MONICA • CALIFORNIA

eh

RAOP 10
Rev. 6/21/49

CONCERNING COMPOUND RANDOMIZATION IN THE BINARY SYSTEM

By John E. Walsh

The RAND Corporation

I consider a set of approximately random binary digits obtained by some experimental process. This paper outlines a method of compounding the digits of this set to obtain a smaller set of binary digits which is much more nearly random. The method presented has the property that the number of digits in the compounded set is a reasonably large fraction (say of the magnitude 1/3 or 1/4) of the original number of digits.

If a set of very nearly random decimal digits is required, this can be obtained by first finding a set of very nearly random binary digits and then converting these digits to decimal digits.

The concept of "maximum bias" is introduced to measure the degree of randomness of a set of digits. A small maximum bias shows that the set is very nearly random.

The question of when a table of approximately random digits can be considered suitable for use as a random digit table is investigated. It is found that a table will be satisfactory for the usual types of situations to which a random digit table is applied if the reciprocal of the number of digits in the table is noticeably greater than the maximum bias of the table.

2. Introduction and discussion. With the development of the theory of games and the more widespread use of experimental methods for determining approximate distributions for statistics whose probability laws are difficult to obtain analytically, a demand for large sets of random digits has arisen. The problem of obtaining a set of digits which can be considered sufficiently random for the situations to which it would be applied, however, is not an easy one. One approach to this problem consists in obtaining a set of digits by some procedure and then applying tests to this set of digits to determine whether it can be considered satisfactory. Although appropriate choice of the tests may result in acceptance of sets of digits which are suitable for certain special types of situations, this approach is of a negative character and does not prove that a given set of digits is sufficiently random; it merely indicates that this may be the case. What is needed is a constructive approach to the problem, i.e., a method of constructing a set of random digits which can be proved sufficiently random for most applications if certain intuitively acceptable conditions are satisfied. A step in this direction has already been taken by H. Burke Horton in [1] and by H. Burke Horton and R. Tynes Smith III in [2]. This paper presents what is hoped will be another step in this direction.

In this paper, considerations will be limited to the case of binary digits. The reasons for this are twofold:

(a). The method used for compounding the digits yields a sharp upper bound for the maximum bias of the compounded set (i.e., a bound that the maximum bias could actually attain) only for the case of binary digits.

(b). Many of the experimental procedures for obtaining approximately random digits consist in first producing binary digits and then converting to another number base. Thus binary digits are produced directly. Hence, to use the results of this paper, the only modification required in these procedures would be to compound the binary digits before they are converted.

Now let us consider some definitions: A set of random variables each of which can assume only the values 0 and 1 will be referred to as a set of binary digits. For convenience, each of the random variables making up a set of binary digits will be called a binary digit; this is not to be confused with the value obtained for the random variable. The absolute value of the deviation from $\frac{1}{2}$ of the conditional probability that a specified binary digit has the value 0 (or 1) is called the bias of that digit for the given conditions on the remaining digits of the set. The maximum bias of a binary digit is defined to be the maximum of the biases of that digit with respect to all possible conditions on the remaining digits of the set. The maximum bias of the set is the greatest of the maximum biases of the digits of the set. A set of binary digits is said to be random if its maximum bias is zero.

The method used to prove that a set of compounded digits has a sufficiently small maximum bias is somewhat similar to the situation encountered in mathematics where one begins with certain axioms and then draws conclusions. If the axioms are correct, the conclusions are necessarily valid. The first step in the compounding procedure consists in obtaining a set of binary digits by some experimental process (perhaps from a random digit machine which is based on some physical principle). The experimental process is so chosen that there is no doubt that the set of binary digits produced satisfies the two conditions:

(i). The maximum bias of the set is less than or equal to some specified value α ($< \frac{1}{2}$).

(ii). The digits of the set can be arranged in a specified array which has the property that the rows of the array are statistically independent.

On the basis of these two assumptions (which play the same role as the axioms mentioned above), it can be proved that the maximum bias of the resulting compounded set of binary digits never exceeds a specified value which depends on α. Moreover, the upper bound for the maximum bias of the constructed set of binary digits can be made extremely small even for large values of α.

If the experimental process is suitably chosen, conditions (i) and (ii) can be satisfied beyond any doubt. For example, let us consider 1000 people located in different parts of the world and not in contact with each other. Let each person flip an ordinary coin high in the air so that it will land on a flat hard surface, record the result (say 0 for a tail and 1 for a head), and then repeat this procedure until 5000 binary digits are obtained. If α is set equal to 3/10, condition (i) is obviously satisfied for the resulting set of 5,000,000 binary digits. Condition (ii) evidently holds if the array is taken to consist of 1000 rows where each row contains 5000 binary digits obtained from one person.

The ideal choice for α would be the actual maximum bias of the set of binary digits obtained from the experimental process. Then the compounding procedure for obtaining a set of digits with a specified upper bound for the maximum bias would be simplified; also the number of digits in the compounded set would be a larger fraction of the original number of digits. Invariably, however, the properties of the experimental process are not known with sufficient accuracy for obtaining anything but a safe upper bound on the maximum bias of the set of digits produced. This situation is analogous to that of estimating the length of a stick which a very rough measurement has shown to be about 10" long. Although one might be very hesitant to believe that the length of the stick lies between 9.9" and 10.1", the contention that the length lies between 5" and 15" can be accepted with virtual certainty and any logical conclusions based on this contention can also be accepted with virtual certainty.

Given the number of binary digits in a set and the maximum bias of the set, is it possible to determine whether the set is suitable for use as a set of random binary digits? An important consideration in answering this question is the use that is to be made of the set of digits. This must always be taken into account before the suitability of the set can be decided. For example, if no more than 1/1000 of the digits of the set are to be used for any particular situation, the set might be satisfactory for the types of cases to which it would be applied; on the other hand, the set might not be suitable for cases of these types if all the digits of the set are used for each situation. This example calls attention to an important point, namely that the suitability of a set of binary digits depends on the number of digits in the set. Let a set have a fixed non-zero maximum bias ρ. If the set contains a sufficiently large number N of digits, relations and expressions involving the digits of the set can be found whose probabilities, moments, etc., can differ greatly from the values which would be obtained if the relations were based on the same number of truly random binary digits. As a specific example consider the relation

<u>All the digits of the set have the value zero</u>.

If the reciprocal of the number of digits in the set is of the same order of magnitude or smaller than the maximum bias of the set, the ratio of the probability of this expression to its hypothetical value can differ noticeably from unity. Thus, at least in certain special cases, a necessary condition for the suitability of a set of binary digits is that $1/N > > \rho$. This condition, however, is also sufficient for most situations to which a set of random digits would be applied. The approximate sufficiency of the condition is a direct consequence of the fact that any set of N binary digits can be considered as a sample value from an N-dimensional population consisting of 2^N discrete points. The $1/N > > \rho$ restriction implies that the probability concentrated at each of the 2^N points is very nearly equal to the hypothetical value of $\left(\frac{1}{2}\right)^N$ for all possible conditions on the remaining digits of the set.

The $1/N > > \rho$ condition is very satisfactory from the viewpoint of probabilities. The probability of any relation based on a subset of the digits of the set (possibly conditioned on other digits from the table) can be interpreted as the sum of the probabilities of those points included in a certain region (defined by the relation) of the N-dimensional probability space of the set of digits. By expanding $(\frac{1}{2} \pm \rho)^N$ it can be shown that the ratio of the probability of any relation based on one or more digits from the set to the corresponding value for a truly random set of digits will be very nearly equal to unity if $1/N > > \rho$.

It is evident that the higher order moments of an expression based on one or more digits of the set can differ noticeably from its hypothetical value even if $1/N > > \rho$; any deviation from the ideal situation, no matter how small, can become important for high order moments. For the first few moments, however, deviations from the hypothetical values are not appreciable since these moments are based on the probabilities at the 2^N points in the N-dimensional probability space and these probabilities are very nearly equal to the hypothetical value of $\left(\frac{1}{2}\right)^N$ in all cases.

The above discussion shows that the values of N and ρ are sufficient to determine whether a set of binary digits is suitable for use as random binary digits for a wide variety of situations. Analogous considerations apply for digits to any number base.

A magnitude definition of the relation $1/N > > \rho$ is difficult to specify. If ρ is the upper bound for the maximum bias of a set of digits obtained by the compounding procedure outlined in this paper, however, it seems that a reasonable condition would be that $1/N \geq 50\rho$. This condition implies that the probability of any relation based on digits of the set can not differ from its hypothetical value by more than approximately 4%. In most practical applications the value obtained for ρ would be noticeably greater than the true value of the maximum bias of the compounded set.

Since the maximum number of digits which can be taken from a table is the total number of digits in the table, the above considerations suggest that a random digit table should be constructed so that the reciprocal of the number of digits in the table is noticeably greater than the maximum bias of the table. Any table having this property would be satisfactory for most situations to which it would be applied.

Now let us consider two different compounding methods which produce sets of binary digits with the same upper bound for the maximum bias. If the computational difficulties of applying the two methods are of comparable magnitudes, it seems reasonable to prefer the method which yields the larger set of digits. For example, if the number of digits in the set obtained by the first method is only 1/8 of the original number of digits while the number in the set obtained by the second method is 1/3 of the original number, the second method would seem preferable even if it required as much as 100% more computation. The compounding method presented in this paper has the property that the number of digits in the compounded set can be held to a reasonably large fraction of the original number of digits at the same time that the upper bound for the maximum bias is made extremely small. The method presented by Horton in [1] does not have this property. For example, let $\alpha = 1/10$. Applying Horton's method, when the compounded set consists of 1/8 of the original number of digits the upper bound for the maximum bias is 12.8×10^{-7}. The example presented in section 3, however, shows that a compounded set whose number of digits equals 1/3 of the original number and which has an upper limit of 11.7×10^{-7} for the maximum bias can be obtained using the method presented in the next section.

Although the compounding method outlined in section 3 is presented as a series of steps, the value of a digit of the compounded set can be written as a linear function (mod 2) of digits of the original set. This was not done in what follows because of the complicated nature of the general form of such expressions. In any particular case, however, these expressions can be written without much trouble and the compounded digits computed from the original digits in a single step.

3. Outline of compounding method and statement of theorems. This section contains a description of the compounding method mentioned in the preceding two sections as well as statements of the basic theorems concerning this compounding method. Proofs of the results stated in this section are given in section 4.

Let us consider the array of mn binary digits

$$(1) \qquad \begin{matrix} x_{11}, x_{12}, \cdots, x_{1n} \\ x_{21}, x_{22}, \cdots, x_{2n} \\ \vdots \quad \vdots \qquad \vdots \\ x_{m1}, x_{m2}, \cdots, x_{mn} \end{matrix}$$

which satisfies conditions (i) and (ii); i.e., the maximum bias of the set (1) is less than or equal to α while a digit x_{uv} is independent of a digit x_{rs} if $r \neq u$ (if $r = u$, however, x_{uv} is not necessarily independent of x_{rs}).

Let a new set of $(m-1)n$ binary digits

$$(2) \qquad y_{ij}, \qquad (i = 1,\cdots,m-1;\ j = 1,\cdots,n)$$

be formed as follows:

$$y_{ij} = x_{mj} + x_{ij} \pmod 2, \quad (i = 1,\cdots,m-1;\ j = 1,\cdots,n).$$

Then the biases of the y_{ij} have the properties

Theorem 1. Let U be a specified set of t-1 of $y_{ij},\cdots, y_{(i-1)j}, y_{(i+1)j},\cdots, y_{(m-1)j}$, $(1 \leq t \leq m-1)$, while V is a specified set of zero or more of the y_{pq}'s with $q \neq j$. Also let Θ consist of the set of integers such that $p \in \Theta$ if $y_{pj} \in U$. Then, if γ_u = maximum bias for the set $x_{u1},\cdots,x_{un}$, $(u = 1,\cdots,n)$,

$$\left|\Pr(y_{ij} = 0 \mid U, V) - \tfrac{1}{2}\right| \leq \gamma_i \left[1 - \prod_{k\in\Theta}\left(\tfrac{1}{2} - \gamma_k\right)/\left(\tfrac{1}{2} + \gamma_k\right)\right]\Big/\left[1 + \prod_{k\in\Theta}\left(\tfrac{1}{2} - \gamma_k\right)/\left(\tfrac{1}{2} + \gamma_k\right)\right]$$

for all possible selections of U, V and of the values for the digits of these sets.

Corollary 1. If exactly t-1 of $y_{1j},\cdots,y_{(i-1)j}, y_{(i+1)j},\cdots,y_{(m-1)j}$ have known values, the maximum bias of the binary digit y_{ij} is less than or equal to

$$\alpha\left[1 - \left(\tfrac{1}{2} - \alpha\right)^t/\left(\tfrac{1}{2} + \alpha\right)^t\right]\Big/\left[1 + \left(\tfrac{1}{2} - \alpha\right)^t/\left(\tfrac{1}{2} + \alpha\right)^t\right].$$

Corollary 2. The maximum bias of the set (2) is less than or equal to

$$\alpha\left[1 - \left(\tfrac{1}{2} - \alpha\right)^{m-1}/\left(\tfrac{1}{2} + \alpha\right)^{m-1}\right]\Big/\left[1 + \left(\tfrac{1}{2} - \alpha\right)^{m-1}/\left(\tfrac{1}{2} + \alpha\right)^{m-1}\right].$$

The basic operation in the method of compounding binary digits is outlined in the procedure given for obtaining the y_{ij} from the x_{uv}. Let $m = (1+t_1)\cdots(1+t_K)$. Then a set of $t_1\cdots t_K n$ binary digits can be obtained from the original set of mn digits x_{uv} by continually applying this basic procedure. The first step consists in dividing the rows of (1) into $(1+t_2)\cdots(1+t_K)$ sets each consisting of $(1+t_1)$ rows in some specified fashion.

Each of these sets is an array of $(1+t_1)$ x n binary digits for which the rows are independent. Apply the method used to obtain the y_{ij} from the x_{uv} to each $(1+t_1)$ x n array separately. Then each array yields a set of $t_1 n$ binary digits and there are $(1+t_2)\cdots(1+t_K)$ such sets. In each set arrange the $t_1 n$ digits into a single row in some specified manner. This furnishes a new array of $[(1+t_2)\cdots(1+t_K)]$ x $[t_1 n]$ binary digits for which the rows are independent. Repeat this procedure with respect to t_2 thus obtaining a new array of $[(1+t_3)\cdots(1+t_K)]$ x $[t_1 t_2 n]$ binary digits for which the rows are independent; etc., until a $(1+t_K)$ x $(t_1\cdots t_{K-1} n)$ binary digit array for which the rows are independent is obtained. Then form a set of binary digits Y_{gh}, $(g = 1,\cdots,t_K;\ h = 1,\cdots, t_1\cdots t_{K-1} n)$, from this array in exactly the same manner that the y_{ij} were obtained from the x_{uv}. Then the biases of the Y_{gh} have the properties

Theorem 2. Let $\beta_0, \beta_1,\cdots, \beta_K$ be defined by $\beta_0 = \alpha$ and

$$\beta_w = \beta_{w-1}\left[1 - \left(\tfrac{1}{2} - \beta_{w-1}\right)^{t_w}/\left(\tfrac{1}{2} + \beta_{w-1}\right)^{t_w}\right]/\left[1 + \left(\tfrac{1}{2} - \beta_{w-1}\right)^{t_w}/\left(\tfrac{1}{2} + \beta_{w-1}\right)^{t_w}\right], \quad (w = 1,\cdots, K).$$

Then, if exactly t-1 of $Y_{1h},\cdots,Y_{(g-1)h}, Y_{(g+1)h},\cdots,Y_{t_K h}$ have known values, $(1 \le t \le t_K)$, the maximum bias of the digit Y_{gh} is less than or equal to

$$\beta_{K-1}\left[1 - \left(\tfrac{1}{2} - \beta_{K-1}\right)^{t}/\left(\tfrac{1}{2} + \beta_{K-1}\right)^{t}\right]/\left[1 + \left(\tfrac{1}{2} - \beta_{K-1}\right)^{t}/\left(\tfrac{1}{2} + \beta_{K-1}\right)^{t}\right].$$

In particular, the maximum bias of the entire set of Y_{gh} is less than or equal to β_K. Also

$$\beta_{K-1}\left[1 - \left(\tfrac{1}{2} - \beta_{K-1}\right)^{t}/\left(\tfrac{1}{2} + \beta_{K-1}\right)^{t}\right]/\left[1 + \left(\tfrac{1}{2} - \beta_{K-1}\right)^{t}/\left(\tfrac{1}{2} + \beta_{K-1}\right)^{t}\right]$$

(3)

$$\le 2^{2^{K-1}} \cdot t \cdot t_{K-1}^2 \cdot t_{K-2}^4 \cdots t_2^{2^{K-2}} \cdot t_1^{2^{K-1}} \cdot \alpha^{2^K}.$$

The inequality (3) is frequently useful from a computational viewpoint. Although the right hand side of (3) is usually noticeably greater than the left hand side, in many cases this rough upper bound is itself small enough to show that the upper bound for the maximum bias is of the desired order of magnitude.

If the set of compounded digits is to be used for a random binary digit table, Theorem 2 shows that advantage can be taken of the position of the digits in the table. Let $M = t_1\cdots t_{K-1} n$ and enter the values of the Y_{gh}, $(g = 1,\cdots,t_K;\ h = 1,\cdots,M)$, into the table in the order

$$Y_{11}, Y_{12}, \cdots, Y_{1M}, Y_{21}, \cdots, Y_{2M}, Y_{31}, \cdots, Y_{t_K 1}, \cdots, Y_{t_K M}.$$

Then, if a set of digits is taken from this table in consecutive order (Y_{11} follows $Y_{t_K M}$), the upper bound for the maximum bias of this set is dependent on the number L of digits in the set. From Theorem 2, the maximum bias of a set of L digits taken in consecutive order from a table formed in this manner is less than or equal to

$$\beta_{K-1}\left[1 - \left(\tfrac{1}{2} - \beta_{K-1}\right)^t / \left(\tfrac{1}{2} + \beta_{K-1}\right)^t\right] / \left[1 + \left(\tfrac{1}{2} - \beta_{K-1}\right)^t / \left(\tfrac{1}{2} + \beta_{K-1}\right)^t\right]$$

for values of L such that $(t-1)M < L \leq tM$, where $1 \leq t \leq t_K$. Thus, if a small set of digits is taken from this table in consecutive order, the upper bound for the maximum bias of this set will usually be noticeably smaller than the upper bound for the maximum bias of the table. Since many uses of a random digit table require only a small fraction of the total number of entries in this table, this property would seem to be desirable. It should be emphasized, however, that the maximum bias of a set taken from this table is always less than or equal to β_K irrespective of the positions that the digits of the sets occupy in the table. Thus nothing is lost by constructing the table in this manner but something can be gained for small sets if the digits are taken from the table in consecutive order.

Now let us consider situations in which it is required that the number of digits in the compounded set is at least a specified fraction, say 1/C, of the original number mn of binary digits. This requires that K and $t_1,\cdots,t_K$ be chosen so that

$$t_1\cdots t_K/(1+t_1)\cdots(1+t_K) \geq 1/C.$$

Also, for given values of K and C, it seems preferable to choose $t_1,\cdots,t_K$ so that the value of β_K is at least approximately minimized. Examination of the results of Theorem 2 indicates that a reasonable method of determining the values of $t_1,\cdots,t_K$ with this in mind consists in first choosing t_1 as small as possible, then (given the value of t_1 equal to its minimum value) choosing t_2 as small as possible, etc. This method is also recommended by the fact that the resulting values of $t_1,\cdots,t_K$ are readily determined. The explicit procedure for finding $t_1,\cdots,t_K$ is given by

Theorem 3. Let the values of the integer K and the constant C (> 1) be given and consider the integers $t_1,\cdots,t_K$ subject to the condition

$$t_1\cdots t_K/(1+t_1)\cdots(1+t_K) \geq 1/C.$$

The minimum value of t_1 is the smallest integer satisfying

$$t_1 > 1/(C-1).$$

In general, $2 \leq w \leq K-1$, having already determined $t_1,\cdots,t_{w-1}$ as their minimum values, the value of t_w is the smallest integer satisfying

$$t_w > 1/\left[Ct_1\cdots t_{w-1}/(1+t_1)\cdots(1+t_{w-1}) - 1\right] .$$

Finally, given $t_1,\cdots,t_{K-1}$ as their minimum values, the minimum value of t_K is the smallest integer satisfying

$$t_K \geq 1/\left[Ct_1\cdots t_{K-1}/(1+t_1)\cdots(1+t_{K-1}) - 1\right] .$$

Now consider the general situation encountered in the application of the compounding process outlined above. Here the values of α, C are given and it is required to choose K and $t_1,\cdots,t_K$ so that the upper bound for the maximum bias of the compounded set of $t_1\cdots t_K n$ binary digits Y_{gh} is less than or equal to a specified value b. The following procedure furnishes a method of solving this problem:

Let K = 1, obtain t_1 according to Theorem 3, and then compute β_1. If $\beta_1 \leq b$, a solution has been obtained. If $\beta_1 > b$, let K = 2 and repeat the procedure to obtain β_2. If $\beta_2 \leq b$, the values of t_1, t_2 and K = 2 are a solution. If $\beta_2 > b$, repeat the procedure for K = 3; etc. In practical situations, the value of K is usually bounded (e.g., by independence properties of the original set of digits). If β_K is still greater than b for the maximum permissible value of K, no solution is obtained. This means that either b must be increased or 1/C decreased or both if a solution is to be found. In many cases, a large amount of computation can be avoided by using the inequality (3). For marginal situations, however, a solution may be missed by using (3) instead of computing β_K.

Example of method. The following table represents an example of application of the above method:

$\alpha = 1/10$	$1/C = 1/3$	$b = 2 \times 10^{-6}$
$K = 1,\ t_1 = 1$		$\beta_1 = 2 \times 10^{-2}$
$K = 2,\ t_1 = 1,\ t_2 = 2$		$\beta_2 \leq 1.6 \times 10^{-3}$
$K = 3,\ t_1 = 1,\ t_2 = 3,\ t_3 = 9$		$\beta_3 \leq 1.04 \times 10^{-4}$
$K = 4,\ t_1 = 1,\ t_2 = 3,\ t_3 = 10,\ t_4 = 44$		$\beta_4 \leq 1.17 \times 10^{-6}$.

Thus $K = 4,\ t_1 = 1,\ t_2 = 3,\ t_3 = 10,\ t_4 = 44$ is a solution.

4. Derivations. The purpose of this section is to furnish proofs of the results stated in the preceding sections.

4.1 Proof of Theorem 1. Let us consider the conditional probability that an arbitrary but fixed y_{ij} has a specified value when the values of a fixed subset of zero or more of the remaining y's are known. For convenience, assume that y_{11} is the binary digit considered and that

values of $y_{21}, y_{31}, \cdots, y_{t1}$ (where t is a fixed integer such that $1 \leq t \leq m-1$) and a set re given while the values of the remaining y's are unknown. Here S represents an arbitrary fixed set of zero or more of the y_{ij}'s for which $j \geq 2$ while $t = 1$ has the interpretation t none of the y_{i1}, $(i \geq 2)$, are given. Let

$$\Pr(x_{m1} = 0|S) = \tfrac{1}{2} + \alpha_{t+1} \quad \text{and} \quad \Pr(x_{k1} = b_k|S) = \tfrac{1}{2} + \alpha_k, \qquad (k = 1, \cdots, t).$$

n, using the independence conditions satisfied by the x's,

$$\Pr(y_{11} = b_1 | y_{21} = b_2, \cdots, y_{t1} = b_t; S)$$

$$= \left[\prod_{k=1}^{t+1} \left(\tfrac{1}{2} + \alpha_k\right) + \prod_{k=1}^{t+1} \left(\tfrac{1}{2} - \alpha_k\right)\right] \Big/ \left[\prod_{k=2}^{t+1} \left(\tfrac{1}{2} + \alpha_k\right) + \prod_{k=2}^{t+1} \left(\tfrac{1}{2} - \alpha_k\right)\right]$$

$$= \tfrac{1}{2} + \alpha_1 \left[\prod_{k=2}^{t+1} \left(\tfrac{1}{2} + \alpha_k\right) - \prod_{k=2}^{t+1} \left(\tfrac{1}{2} - \alpha_k\right)\right] \Big/ \left[\prod_{k=2}^{t+1} \left(\tfrac{1}{2} + \alpha_k\right) + \prod_{k=2}^{t+1} \left(\tfrac{1}{2} - \alpha_k\right)\right]$$

$$= \tfrac{1}{2} + \alpha_1 \delta.$$

$|\delta| = (1-P)/(1+P)$ if $0 \leq P \leq 1$ and equals $(P-1)/(1+P)$ if $P > 1$, where $P = \prod_2^1 \left(\tfrac{1}{2} - \alpha_k\right)/\left(\tfrac{1}{2} + \alpha_k\right)$. Let γ_u be the maximum bias for the set of binary digits $x_{u1}, \cdots, x_{un}$, $= 1, \cdots, m)$. Then it is easily seen that

$$\max_P |\delta| \leq \left[1 - \prod_{k=2}^{t+1} \left(\tfrac{1}{2} - \gamma_k\right)/\left(\tfrac{1}{2} + \gamma_k\right)\right] \Big/ \left[1 + \prod_{k=2}^{t+1} \left(\tfrac{1}{2} - \gamma_k\right)/\left(\tfrac{1}{2} + \gamma_k\right)\right].$$

us

$$\left|\Pr(y_{11} = b_1 | y_{21} = b_2, \cdots, y_{t1} = b_t; S) - \tfrac{1}{2}\right|$$

$$\leq \gamma_1 \left[1 - \prod_{k=2}^{t+1} \left(\tfrac{1}{2} - \gamma_k\right)/\left(\tfrac{1}{2} + \gamma_k\right)\right] \Big/ \left[1 + \prod_{k=2}^{t+1} \left(\tfrac{1}{2} - \gamma_k\right)/\left(\tfrac{1}{2} + \gamma_k\right)\right]$$

or all possible selections of $b_1, \cdots, b_t$ and all possible selections of S and the values for ie digits of S. It is to be observed that this inequality is valid for $t = 1$.

Evidently this result can be modified to apply to an arbitrary y_{ij} for which t-1 of $1j, \cdots, y_{(i-1)j}, y_{(i+1)j}, \cdots, y_{(m-1)j}$ have given values. This obvious modification results in heorem 1.

4.2 Proof of Theorem 2. By Corollary 2, the maximum bias of the $[(1+t_2)\cdots(1+t_K)] \times [t_1 n]$ array is less than or equal to β_1. In general, $2 \le w \le K$, by Corollary 2, the maximum bias of the $[(1+t_{w+1})\cdots(1+t_K)] \times [t_1 \cdots t_{wn}]$ array is less than or equal to β_w. Finally, by Corollary 1, if exactly t-1 of $Y_{1h},\cdots,Y_{(g-1)h}, Y_{(g+1)h},\cdots,Y_{t_K h}$ have known values, $(1 \le t \le t_K)$, the maximum bias for the binary digit Y_{gh} is less than or equal to

$$\beta_{K-1}\left[1 - \left(\tfrac{1}{2} - \beta_{K-1}\right)^t / \left(\tfrac{1}{2} + \beta_{K-1}\right)^t\right] \Big/ \left[1 + \left(\tfrac{1}{2} - \beta_{K-1}\right)^t / \left(\tfrac{1}{2} + \beta_{K-1}\right)^t\right].$$

The inequality (3) is an immediate consequence of the relation

$$\alpha\left[1 - \left(\tfrac{1}{2} - \alpha\right)^s / \left(\tfrac{1}{2} + \alpha\right)^s\right] \Big/ \left[1 + \left(\tfrac{1}{2} - \alpha\right)^s / \left(\tfrac{1}{2} + \alpha\right)^s\right] \le 2s\alpha^2 .$$

4.3 Proof of Theorem 3. From the given condition

$$t_K \ge 1 \Big/ \left[Ct_1 \cdots t_{K-1}/(1 + t_1)\cdots(1 + t_{K-1}) - 1\right].$$

From this inequality for t_K it follows that

$$Ct_1 \cdots t_{K-1}/(1 + t_1)\cdots(1 + t_{K-1}) - 1 > 0.$$

Thus

$$t_{K-1} > 1 \Big/ \left[Ct_1 \cdots t_{K-2}/(1 + t_1)\cdots(1 - t_{K-2}) - 1\right].$$

In general, $3 \le w \le K-1$, given

$$t_w > 1 \Big/ \left[Ct_1 \cdots t_{w-1}/(1 + t_1)\cdots(1 + t_{w-1}) - 1\right]$$

it follows that

$$Ct_1 \cdots t_{w-1}/(1 + t_1)\cdots(1 + t_{w-1}) - 1 > 0$$

whence

$$t_{w-1} > 1 \Big/ \left[Ct_1 \cdots t_{w-2}/(1 + t_1)\cdots(1 + t_{w-2}) - 1\right].$$

Finally

$$t_1 > 1/(C - 1).$$

REFERENCE

[1] H. Burke Horton, "A method for obtaining random numbers," Annals of Math. Stat., Vol. 19 (1948), pp. 81-85.

[2] H. Burke Horton and R. Tynes Smith III, "A direct method for producing random digits in any number system," Annals of Math. Stat., Vol. 20 (1949), pp. 82-90.